Institution: University of Northumbria at Newcastle

Unit of Assessment: 11 (Computer Science and Informatics)

Title of case study: Reducing the risk of cybercrime through human-centred cybersecurity

Period when the underpinning research was undertaken: 2013 – 2019		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s):	**Role(s) (e.g. job title):**	**Period(s) employed by submitting HEI:**
James Nicholson	Lecturer	2010 – present
Period when the claimed impact occurred: 2014 – 2020		
Is this case study continued from a case study submitted in 2014? N		

1. Summary of the impact (indicative maximum 100 words)

Cybercrime is a growing national problem, and the 'human factor' is a key cybersecurity vulnerability. Northumbria Cyber Security Research Group (NCSRG), recognised as an 'Academic Centre of Excellence in Cybersecurity' in 2019, is a cross-faculty, multi-disciplinary group investigating human-centred approaches to cybersecurity. NCSRG's research has informed key cybersecurity policy documents in the UK and was used by the National Cyber Security Centre for campaigns raising public awareness of cybercrime. Through collaboration with industry (Think Cyber), the NCSRG contributed to the development of an award-winning cybersecurity training product that has been used to train staff at Tesco Bank and the London Borough of Camden Council. Cybersecurity awareness of over 1,000 older people (a group considered amongst the most vulnerable to cybercrime) in the North East of England has been increased through the work of the NCSRG with the University of the Third Age. [text removed for publication]

2. Underpinning research (indicative maximum 500 words)

Cybercrime costs the UK economy billions of pounds per year. Northumbria Cyber Security Research Group (NCSRG) is a cross-faculty, multi-disciplinary group which aims to understand security vulnerabilities which exist at the intersection of people, technology, and place. The group includes Dr James Nicholson from the Department of Computer and Information Sciences, as well as Professor Pamela Briggs and Professor Lynne Coventry from the Department of Psychology, and others. The group combines technical computer science expertise on such topics as web security protocols and image recognition, with human-centred work on security, privacy, and trust. Nicholson contributes the technical knowledge of digital security mechanisms and countermeasures while investigating the opportunities to improve user-facing technologies.

Most common cybersecurity measures rely on simple authentication mechanisms, such as password or face recognition, that are not always effective in stopping cybercrime. In 2013, NCSRG's research explored the experiences of older users with text passwords [**R1**], showing that knowledge-based authentication methods (passwords and PINs) were problematic for older people, due to such factors as memory decline. This work demonstrated the importance of tailoring technology to distinct population groups. As a result, the NCSRG team developed more inclusive authentication systems that could benefit both older and younger users by improving the practical entropy of codes without compromising their memorability [**R1**].

With the objective of creating secure online systems that account for human behaviour, NCSRG also looked into the design of user interfaces during the EPRSC-funded Choice Architecture for Information Security (ChAISe) project. The team investigated a choice architecture (an approach to retaining a user's right to choose while 'nudging' them to make certain choices) as a mechanism for bridging the technical security countermeasures of organisations and human limitations, by carefully designing user-facing security interfaces [**R2**]. The effectiveness of 'nudges' in helping users to identify social engineering attacks was evaluated, showing that

users were more successful in identifying phishing emails when their attention was drawn to the sender's details (name and originating email address). This work highlighted the fact that interfaces hiding sender information in emails (e.g., full originating email address) is problematic and potentially hinders users' efforts to evaluate the authenticity of emails in their everyday lives. While investigating methods to improve cybersecurity, the NCSRG showed that a simple 'nudge' towards protective actions (e.g., a message reminding a user to create a stronger password) can significantly improve security protections [**R3**]. Refining their work on 'nudges', NCSRG researched cybersecurity in the workplace by creating a gamified method of detecting cybersecurity vulnerabilities. This work revealed tensions between corporate approaches to cybersecurity compliance and the attitudes and behaviours of employees [**R4**]. This research showed how online tools can inform the design of successful campaigns and training events that can improve the socio-technical security of organisations.

The common thread running through NCSRG's research has established that systems designed with diverse communities of users in mind, lead to more secure interactions and better cybersecurity protection. In 2017, in collaboration with the Universities of Bath, Cranfield, and Portsmouth, Northumbria's team started working on the Cybersecurity Across the Lifespan (cSALSA) project, which focused on age-related vulnerabilities. This work built on NCSRG's earlier research into difficulties that older adults (and other communities) experience when trying to authenticate their identity (e.g., using passwords and PINs) [**R1**]. The research found that older people are amongst the most vulnerable to cybercrime, yet they are also the least likely to use online learning sources to increase cybersecurity literacy [**R5**]. The cSALSA project examined the most effective methods of communicating cybersecurity information to older adults, identifying training opportunities and technologies that could facilitate better understanding of these technical concepts [**R5**]. In 2019, NCSRG used this research to develop an EPSRC NetworkPlus funded CyberGuardians project, designed to create community-based cybersecurity courses in the North East of England, as an intervention to increase cybersecurity awareness.

Acknowledging NCSRG's innovative work in human-centred cybersecurity, in 2019 the National Cyber Security Centre (NCSC, the UK's technical authority for cyber threats) designated Northumbria University as an 'Academic Centre of Excellence in Cybersecurity'.

3. References to the research (indicative maximum of six references)

R1. James Nicholson, Coventry*, L., and Briggs*, P. (**2013**) 'Faces and pictures: Understanding age differences in two types of graphical authentications' *International Journal of Human-Computer Studies* **71**(10): 958-966 https://doi.org/10.1016/j.ijhcs.2013.07.001

R2. James Nicholson, Coventry*, L., and Briggs*, P. (**2017**) 'Can we fight social engineering attacks by social means? Assessing social salience as a means to improve phish detection' *Proceedings of the Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)* https://www.usenix.org/system/files/conference/soups2017/soups2017-nicholson.pdf. Available on request. Papers submitted undergo three rounds of peer review with c.20% acceptance

R3. James Nicholson, Vlachokyriakos**, V., Coventry*, L., Briggs*, P., and Olivier*, P. (**2018**) 'Simple nudges for better password creation' *Proceedings of the 32nd International BCS Human Computer Interaction Conference* https://www.scienceopen.com/document_file/7cd84218-d1d8-424c-94ce-87b1efff6c03/ScienceOpen/BHCI-2018_Nicholsona.pdf. Available on request

R4. James Nicholson, Coventry*, L., and Briggs*, P. (**2018**) 'Introducing the cybersurvival task: assessing and addressing staff beliefs about effective cyber protection' *Proceedings of the Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* https://www.usenix.org/system/files/conference/soups2018/soups2018-nicholson.pdf Available on request. Papers submitted undergo three rounds of peer review with c.20% acceptance

R5. James Nicholson, Coventry*, L. and Briggs*, P. (**2019**) 'If it's important it will be a headline: Cybersecurity information seeking in older adults' *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*: 1-11 https://doi.org/10.1145/3290605.3300579

*Internal Northumbria co-authors: L. Coventry and P. Briggs (UoA 4 - Psychology)
**External university co-authors: V. Vlachokyriakos (University of Newcastle) and P. Olivier (Monash University, Australia), J. Vila (University of Valencia, Spain)

4. Details of the impact (indicative maximum 750 words)

Northumbria Cyber Security Research Group (NCSRG) achieved impact in three spheres: informed national cybersecurity policy documents and national campaigns; contributed to the development of the commercial cybersecurity training tools that were utilised with private and public organisations; and raised awareness of cybercrime among over 1,000 older people (vulnerable to cybercrime group) in the North East of England, through novel peer-to-peer training courses.

4.1. Contribution to cybersecurity policy development and national campaigns in the UK
NCSRG directly informed the government's approach to cybersecurity in the UK. In 2014, NCSRG members were invited to contribute to a report by the UK Government Chief Scientific Adviser on 'The Internet of Things: making the most of the Second Digital Revolution' [**E1**, Northumbria's contribution is acknowledged on p38]. The report set out a vision for the Government's regulation of data flows created by Internet of Things (IoT) technologies, and the research agenda outlined in that report led directly to the establishment of the GBP14,000,000 PETRAS National Centre of Excellence for IoT Systems Cybersecurity in 2018. PETRAS considers issues of privacy, ethics, trust, reliability, acceptability, and security [i.e., human-centred aspects of cybersecurity analysed in **R1**, **R4**, **R5**] as they relate to IoT devices, systems, and networks. The centre is comprised of a consortium of 16 research institutions, including Northumbria University [**E2**]. Through collaboration with industry and government partners, PETRAS ensures that research is directly applied to benefit society, business, and the economy.

NCSRG also shaped national guideline recommendations on the IoT. In 2018, NCSRG joined an academic and industry panel created by the UK Government's Department for Digital, Culture, Media and Sport (DCMS), to assess how best to ensure that consumer internet-connected products and associated services are secure. The DCMS report 'Secure by Design: Improving the cyber security of consumer Internet of Things' explicitly acknowledged the influence of the cSALSA [**R5**] project as the source of findings that helps Government *'to design more effective cyber security advice and educational materials that are tailored for different audiences'* [**E3**, p27].

While informing key UK policy documents on cybersecurity, Northumbria's work also shaped cybersecurity campaigns run by the National Cyber Security Centre, a branch of the Government Communications Headquarters, responsible for improving the security of the UK's online activity through technological improvements and advice to citizens and organisations. National campaigns run since 2015, including 'People are the strongest link', 'You shape security', and 'Cyber Aware Campaign', embedded NCSRG's findings on how to make cybersecurity available to various groups [**R1**, **R5**], such as senior citizens and employees of private and public organisations [**E4**].

4.2. Development of novel cybersecurity training products
NCSRG's work became a key part of award-winning cybersecurity training products developed by an external company, Think Cyber, which were used by customers including Tesco Bank and the London Borough of Camden Council. In 2018, NCSRG's research [**R2**, **R4**, **R5**] was used to improve Think Cyber's Redflags™ product. Tim Ward, CEO and Co-founder of the Think Cyber, stated:

'[Collaboration with Northumbria] highlighted some key do's and do not's for delivering security awareness that have formed a significant part of our marketing and the narrative behind our unique approach to security awareness: little and often, easy to access, simple and actionable, context driven/real time. Redflags™, the product that incorporates this work has recently [2020] won the SC Award for Best Professional Training Programme' [**E5**].

Following the refinement of the existing Redflags™ product, Think Cyber and NCSRG secured GBP40,000 Innovate UK funding to create novel cybersecurity awareness training. The need to increase cybersecurity awareness is partly driven by regulations (e.g., ISO027001, EU NIS Directive) requiring companies to include cybersecurity courses in their programmes of staff training. The new training product developed in collaboration with Northumbria (built on **R2** and **R4**) [**E5**] recognised both the needs and behaviours of the staff who receive such training, and the requirements of enterprise practitioners who are responsible for delivering the training to staff. Tim Ward, CEO and Co-founder of the Think Cyber, stated:

'[We] established problems with existing training and how it could be improved. We also evaluated the design of four potential approaches that we considered developing in the future. Two particular ideas from this – Security Bulletins and Real-time tips have evolved into key parts of our product. We are now marketing a NCSC certified set of Security Bulletins (now named "Stories") and have deployed a bespoke version of this to Tesco Bank and Camden Council [text removed for publication]' [**E5**].

NCSRG helped the company to develop a strategic vision for their products and to secure an excellent reputation in the field of cybersecurity training [**E5**]. The company was selected for the first cohort of the technology innovation accelerator 'London Office for Rapid Cybersecurity Advancement' and was one of only seven (and only two outside the US) finalists in the New York City Mayor's Cyber Moonshot Challenge [**E5**].

4.3. Reducing the risk of cybercrime targeting older people
Older people form a population group that is amongst the most vulnerable to cybercrime. Many senior citizens are aware of online risks but are often not sure how to protect themselves, which sometimes impedes their use of online tools altogether. In the North East of England, the NCSRG team enhanced the cybersecurity awareness of over 1,000 older people [**E6**, **E7**].

Working with University of Third Age (U3A) in the North East of England, in 2017 the NCSRG team organised practical workshops that focused on password management, social engineering, online privacy, social media, privacy implications of GDPR, and online shopping and banking for older people [based on research on older people's use of passwords and other authentication methods **R1**, **R5**]. As a result of these workshops, over 240 older people increased their awareness of cybersecurity [**E6**]. Following the workshops, due to positive feedback and high demand, the team decided to create a peer-to-peer programme that would allow members of the community to train their peers in cybersecurity. The innovative CyberGuardians project was launched in 2019 by the NCSRG team in collaboration with the U3A and the Old Low Light Heritage Centre. During the project, NCSRG designed and delivered training to 14 CyberGuardians from across the region (Whitley Bay, Prudhoe, Newcastle, Gateshead, Northallerton, Teesside, Tynemouth) – older people who disseminated cybersecurity messages within their communities. The U3A report stated:

'Up until the end of September 2020, the CyberGuardians helped approximately 820 people with cybersecurity advice and help… This is an amazing achievement for the 14 CyberGuardians, but even more people can still benefit from their knowledge. The CyberGuardians have been particularly active organising training sessions during the current UK Covid-19 lockdown, given the 400% increase in Coronavirus scams during this period, but are looking to continue helping as many people as possible' [**E7**].

Counting the initial cybersecurity workshops and the CyberGuardians' training, over 1,000 hard to reach and vulnerable (to cybercrime) older people in the North East benefitted from NCSRG's work. Mike Martin, former U3A Northumbria Regional Committee Member and a CyberGuardian, stated:

> *'The message of good security practices is better received when it comes from people that they [older people] trust, and it is incredible to see the positive impact that a few individuals have had on the general online protection of older adults in the North East of England. This improved protection and awareness would not have been possible without Northumbria University'* [**E6**].

[text removed for publication]

5. Sources to corroborate the impact (indicative maximum of 10 references)

Ref.	Source of corroboration	Link to claimed impact
E1	Report - 'The Internet of Things: making the most of the Second Digital Revolution' (2014)	Corroborates contribution to cybersecurity policy in the UK
E2	Document - PETRAS website	Corroborates that Northumbria University is 1 of 16 institutions comprising PETRAS
E3	Report - 'Secure by Design' (2018)	Corroborates contribution to cybersecurity policy in the UK
E4	Testimonial - Ceri Goncalves Jones, former Lead for People Centred Security at the NCSC	Corroborates that Northumbria's research has informed national cybersecurity campaigns
E5	Testimonial - Tim Ward, CEO and Co-founder of Think Cyber	Corroborates development of the award-winning cybersecurity training products
E6	Testimonial - Mike Martin, former U3A Northumbria Regional Committee Member, and a CyberGuardian	Corroborates increased awareness in cybersecurity amongst older people in the North East of England
E7	Report - University of Third Age CyberGuardian's project report (2020)	Corroborates increased awareness in cybersecurity amongst older people in the North East of England
E8	Testimonial - Paul Waller, Head of Research at the NCSC	[text removed for publication]